Improving Cyber Situational Awareness in Maritime Surveillance

Jussi Simola and Jyri Rajamäki
Laurea University of Applied Sciences, Research, Design and Innovations, Finland
simolajussi@gmail.com
jyrirajamaki@laurea.fi

Abstract: Maritime surveillance has become one of the main areas in managing overall situational awareness. For example, the growing importance of maritime traffic in cross-border trade has created new pressures to develop new technologies for accident prevention. Maritime safety is also a matter of concern for continuity management. Automatic ship alarm systems, coastal radars and coastal cameras are not alone sufficient equipment to build maritime awareness. The Universal Shipborne Automatic Identification System (AIS) is a ship transponder system that is currently used by most actors in the commercial shipping industry. Ships equipped with an AIS transponder send out a packet every few seconds with data about the ship and its journey. The transponder transmits and receives information on VHF channels. This globally used tracking system is highly vulnerable to hacking. A major maritime traffic problem arises if transponders are switched off. Hybrid threats need coordinated hybrid responses; therefore, a cyber situational picture is also needed. The cyber dimension is an essential part of the management of situational awareness. This study was conducted on the ground by visiting four situation and command centers of the Public Protection and Disaster Relief services located in Southwestern Finland. The main results can be summarized so that the failure to use ship transponders affects misuse of the authorities' technical and physical resources. Also, the lack of real time data from ships with limited data transmission capacity affects the correct formation of the common situational picture—for example, from the site of an accident. The technical communication solutions of the PPDR authorities should be more standardized and management should be more centralized. A hybrid emergency model with emergency response functions is necessary. Currently, the flow of real time data is not being transmitted, for example, from cruise ships to the Maritime Rescue Coordination Centre. The developed Hybrid Emergency Response model is a unique concept that can be transferred to the maritime environment. By using the OSINT (Open Source INTelligence) process in the hybrid emergency model, it is possible to gather meaningful intelligence data related to maritime security. Essential open source information has geospatial dimensions. The main purpose of the study is to enhance maritime safety and create a common intelligent maritime emergency management system for public safety organizations.

Keywords: cyber security, hybrid emergency response, PPDR, OSINT, early warnings

1. Introduction

European governments and the European Public Protection and Disaster Relief services—such as law enforcement, firefighting, medical emergency, disaster recovery and military services, but also voluntary associations like civil protection activity or voluntary firefighters—have recognized that the lack of interoperability of technical systems limits cooperation between authorities.

At the EU level, for example, the Common Information Sharing Environment (CISE), the European Coast Guard Functions Academy Network II (EFGA NET 2), the Early Warning for Increased Situational Awareness (EWISA), Safety Authorities in the Arctic Countries (SARC) and Maritime Integrated Surveillance Awareness (MARISA) are all currently being developed together by the European Commission and EU/EEA Member States (The Finnish Border Guard, 2017, Marisa, 2017).

A domestic strategy plan such as the National CBRNE strategy demonstrates that maritime safety is one of the main focus areas when the purpose is to develop a common situational maritime awareness for different authorities and decision-makers. The overall aim of the strategy is to continuously improve the prevention of and preparedness for CBRNE threats and incidents in order to safeguard society and secure the functions vital to society. CBRNE threats refer to hazardous incidents caused by chemical substances (C), biological pathogens (B), radioactive material (R), nuclear weapons (N) and explosives (E) as well as by the misuse of expertise related to these (CBRNE strategy working group, 2017).

The Finnish Border Guard (including the coast guard services) acts under the authority of the Ministry of the Interior but can be incorporated fully or in part into the defense forces when required by defense readiness. The Finnish Defence Forces also monitors sea areas to detect and locate accidents, abnormal events and emergency phases in conjunction with the surveillance of territorial integrity and participates in SAR operations by providing access to its special expertise, personnel and equipment (Kaukanen, Möttönen, 2010, Ministry of the Interior, 2005).

The Finnish Border Guard ensures the security of Finland and prevents security threats directed towards Finland and Europe at external borders. The Finnish Border Guard has many important tasks. Crime prevention is one of the most important areas. It also takes care of people's safety in the border area and on islands.

Coast guard services may include search and rescue (SAR) at sea and in the air, the protection of coastal waters, criminal interdiction, illegal immigration and disaster and humanitarian assistance in operational areas. These functions may vary according to the administration, but the core functions are generally the same. The Finnish maritime search and rescue (SAR) system is one part of the wider security system of the Finnish Border Guard. The Finnish Border Guard has immediate readiness for management and operations during maritime incidents. The Coast Guard also promotes the protection of the maritime environment and it covers 1,250 kilometers of territorial waters (The Finnish Border Guard, 2018; Kaukanen & Möttönen, 2010; Ministry of the Interior, 2005).

Maritime safety has become one of the main discussion areas between public safety authorities and decision-makers in Europe. Overall situational awareness requires different kinds of technical solutions that can combine and produce correct real time data to support correct decisions. Hybrid threats require a coordinated hybrid response. Therefore, a cyber situational picture is an occasional factor when authorities need to create a common situational picture—for example, from the scene of an accident. If oil tankers were to collide in the Gulf of Finland, the ships could spill up to 30,000 tons of oil into the sea. It is important that the nature of the accident is evaluated as soon as it occurs, and the observer must immediately inform the state leadership of major ship accidents.

2. Theoretical framework

2.1 Maritime situational awareness and new automated and unmanned technology

According to the Ministry of Defence (Ministry of Defence, 2010) situational awareness means the understanding of decision-makers and their advisors of what has happened, the circumstances under which it happened, the goals of the different parties and the possible development of events, all of which are needed to make decisions on a specific issue or range of issues. A general definition of situational awareness is the perception of the elements in the environment within time and space, the comprehension of their meaning and the projection of their status in the near future (Endsley, 1988). "Situational awareness is the ability to identify, process and comprehend the critical information about an incident. It is knowing what is going on around you. Situational awareness requires continuous monitoring of relevant sources of information regarding actual incidents and developing hazards" (Homeland Security, 2008).

According to Franke and Brynielsson (2014), cyber situational awareness is a subset of situational awareness, i.e. cyber situational awareness is the part of situational awareness that concerns the cyber environment.

Communications include sharing and the distribution of information: computer systems; control systems (e.g. supervisory control and data acquisition, SCADA); networks, such as the Internet; and cyber services (e.g. managed security services), which are all part of the cyber infrastructure.

The European Union has funded many unmanned maritime situational awareness projects. It has been seen as a future goal to develop and produce automatic solutions for the maritime environment. Unmanned systems, vessels and aerial vehicles will gradually replace human resources. Such technological development also means that information systems are more vulnerable to different types of threats, such as cyber threats. Therefore, advanced solutions are needed to prevent different kinds of threats. Maritime actors, such as shipbuilders, shipping companies and harbors, would need to ensure that their autonomous vessels are protected against attacks by hackers or pirates. In other cases, new technology faces big problems because the responsibility for maritime traffic is shifting from human actors to automated functions.

Maritime surveillance is understood as the process of watching, monitoring, recording and processing the behavior of people, objects and events in order to control activity. The aspects of maritime surveillance discussed in this paper include border control, safety and security, customs, fisheries control and environmental protection (Kaukanen & Möttönen, 2010).

2.2 Organizational influences in Finnish maritime security

The structural changes within the public sector, such as the regional administration reform, the Emergency Response Centre (ERC) reform and ongoing social welfare and health care reform, have influenced the work processes of public sector employees over the past ten years. Due to the regional administrative reform, preparedness plans also need to be changed.

The Baltic Sea Maritime Incident Response Group (Baltic Sea MIRG) project was established by the Finnish Border Guard as the responsible maritime search and rescue authority in cooperation with Finland's Emergency Rescue Services. MIRG is an international project led by the Finnish Border Guard. The purpose of this is to create a MIRG coordination model and operational guidelines for international MIRG operations and to support the harmonization of MIRG services in Europe (Finnish Border Guard - Finnish Transport Safety Agency, 2016).

The Finnish Border Guard is the lead SAR authority and responsible for coordinating all SAR activity. It has a direct emergency number for emergency situations. Under the Maritime Search and Rescue Act (Ministry of the Interior, 2005), the Finnish Border Guard:

- Is responsible for planning, developing and supervising all SAR activity as well as coordinating cooperation with other public authorities and volunteers.
- Coordinates and conducts search and rescue operations.
- In the event of an emergency, is responsible for coordinating radio communications and facilitating telemedical assistance services between medical care providers and vessels.
- Works to prevent accidents and emergencies.
- Is responsible for the Maritime Assistance Service (MAS).
- Is responsible for receiving all distress signals received from maritime, aviation and private emergency transmitters and conveying such signals to the relevant national authority as well as the national coordination of all COSPAS-SARSAT matters.
- Provides SAR leadership training and other SAR-related education and training.

The Finnish Border Guard takes part in search and rescue operations in its control area by providing the equipment, personnel resources and expert services needed for search and rescue operations if the scale or special nature of the incident makes this necessary. Participation in search and rescue may not endanger performance of the border guard functions and the country's military defense services.

The Finnish Border Guard may perform functions in its control area that are needed to find and assist persons who have got lost in open country or are otherwise in need of immediate assistance there. The responsibility for leading searches for missing persons rests with the police. Separate provisions are laid down on Finnish Border Guard functions as part of the maritime search and rescue service (Ministry of the Interior, 2005a; Ministry of the Interior, 2005b; Ministry of the Interior, 2009).

The Finnish Border Guard may, using its vessels, aircraft and other special vehicles, provide urgent ambulance transport in its control area that the authorities or ambulance service enterprises otherwise handling ambulance transport are unable to perform because they lack the vessels, aircraft or other special vehicles (Ministry of the Interior, 2009; Ministry of The Interior, 2005).

In its control area, the Finnish Border Guard may provide the kind of special transport that the State is required to provide in order to ensure a person's personal safety when no other State authority can provide such transportation. The Finnish Border Guard may also, upon request, give executive assistance to some other authority in its control area that is required by law to perform a control function (Ministry of the Interior, 2005).

2.3 Intelligence solutions for public safety organizations

OSINT is defined as the systematic collection, processing, analysis and production, classification and dissemination of information derived from sources openly available to and legally accessible by the public in response to particular government requirements serving national security. It is any unclassified information, in

any medium, that is generally available to the public, even if its distribution is limited or only available upon payment (Glassman & Kang, 2012; Morrow & Odierno, 2012; Nurmi, 2015).

Most information has geospatial dimensions. Examples of geospatial open source include maps, airborne imagery, atlases, gazetteers, port plans, gravity data, aeronautical data, navigation data, geodetic data, human terrain data (cultural and economic), environmental data, commercial imagery, LIDAR, hyper and multi-spectral data, geo-names and features, urban terrain, vertical obstruction data, boundary marker data, geospatial mashups, spatial databases and web services. Most of the geospatial data mentioned above is integrated, analyzed and syndicated using geospatial software such as a Geographic Information System (GIS) (Morrow & Odierno, 2012; Nurmi, 2015; Trottier, 2015; Vetter, 2015; Wood, 2016).

Social Media Intelligence (SOCMINT) identifies social media content in particular as a challenge and opportunity for open source investigations (Trottier, 2015). Big data includes processes of analysis, capture, research, sharing, storage, visualization and safety of information. Associated with OSINT, Big Data is the ability to map standards of behavior and tendencies (Dos Passos, 2016). The availability of worldwide satellite photography, often of high resolution, on the web (e.g. Google Earth Pro) has expanded open-source capabilities into areas formerly available only to major intelligence services.

2.3.1 Centralized cyber threat detection

One way of examining cyber security content automation is through the generalized functional model in use by the standards community. As illustrated in Figure 2, the security functions contained in this model generally represent the first wave plus a portion of the second wave. Security content automation standards that can facilitate the exchange of information with and among functions are annotated adjacent to each function, input or output. In general, the functions left to right can be organized into “preincident detection” (asset inventory, configuration guidance analysis, vulnerability and threat analysis) (National Protection and Programs Directorate, 2011).

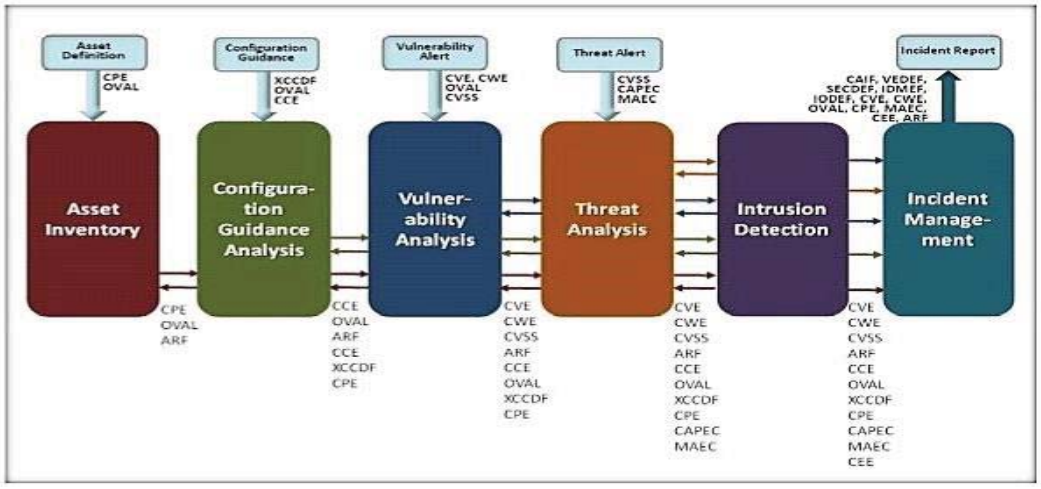

Figure 1: Centralized threat detection system

2.3.2 Multi-layer maritime intelligence system Kingfisher

Kingfisher is based on a multi-sensor, multi-layer maritime intelligence system that combines a variety of information sources to expose the covert movements of vessels and boats. Utilizing Satellite Automatic Identification system (S-AIS) data, Synthetic Aperture Radar satellite imagery, electro-optical satellite imagery, Vessel Monitoring Systems (VMS), coastal radar, open source intelligence (OSINT) and weather patterns, the system is one of the most developed in maritime cyber-physical ecosystems (ISI, 2017).

2.4 Emergency maritime communications

European authorities communicate with each other through the Virve network. There is a need to create a new and trusted network with a wide bandwidth. Transmission capacity is often limited in an overload situation, therefore there is a need to develop new hybrid communication models to utilize real time data.

Shipping in the Baltic Sea, for example, is continuously monitored using AIS tracking. By analyzing historical data regarding vessels, the identity, type, position, speed and traffic intensity can be mapped in detail and provide important input to marine spatial planning. Along with more precise information about the monitored ships and the results of port state controls, AIS data can also make it easier to assess different short- and long-term effects of shipping on the marine environment. There are several AIS tracking websites on the internet that citizens can visit and use (SIME, 2014).

The use of emergency services with the COSPAS-SARSAT satellite system requires an emergency transmitter. Locating an emergency transmitter in emergency situations is much more accurate and faster if the emergency transmitter also includes GPS positioning. Figure 1. illustrates how the COSPAS-SARSAT system works (Secretariat of the Cospas-Sarsat Programme, 2016).

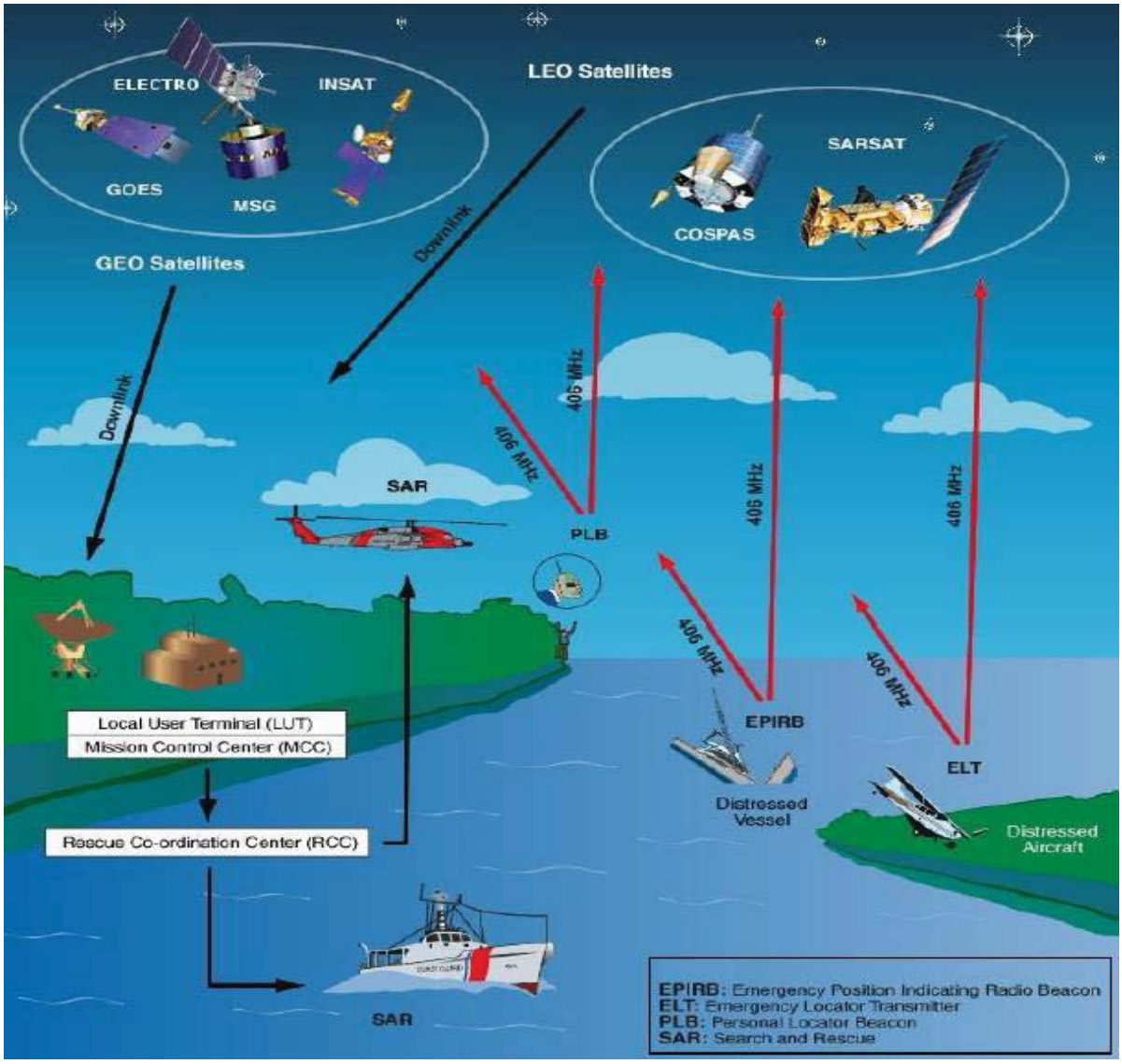

Figure 2: Basics concept of the COSPAS-SARSAT system

2.4.1 SAR suitable equipment

The Finnish Border Guard's vessels and aircraft are used in 70 per cent of all maritime SAR activity in Finland (The Finnish Border Guard, 2018). Patrol vessel *Turva* started operations in 2014. The vessels underwater activities center provides the ability to create an underwater situational picture. Vessels are also identified at the request of other authorities in relation to their needs. With its sensors, *Turva* brings more performance to METO cooperation. The underwater activities center is used to conduct underwater activities. The DP2 classified standby system enables efficient and safe operation at the side of the accident. *Turva's* equipment includes different kinds of systems, such as a 3D radar, thermal camera, searchlight and scanning sonars and modern

ROV equipment. In connection with the use of ROV equipment, the two *Turva* crews have continuous preparedness to use divers. The *Super Puma* together with *Turva* provide quick access to additional information, such as information about identifiable objects or target areas. NVG functions, the Virtual Horizon system and the HVLA (Helicopter Visual Landing Aid) system enable safe cooperation (Simola et al., 2015).

2.5 Distributed Systems Intercommunication Protocol (DSiP)

DSiP enables multiple simultaneous communication channels between the remote end and the control room: if one communication channel is down, other channels will continue to operate. DSiP makes communication reliable and unbreakable by using various physical communication methods in parallel. Applications, equipment and devices can communicate over a single unbreakable data channel. Satellite, TETRA, 2G/3G/4G, VHF radios and other technologies can be used simultaneously. DSiP is simultaneously a protocol-level and routing-level traffic engineering software solution for intelligently handling data routing, using all kinds of physical media, including IP and non-IP communication. The latest innovation is an all-in-one solution DSiP-router-laptop (Rajamäki & Villemson, 2009; Simola & Rajamäki, 2015).

3. Research background, method and process

PPDR authorities are tasked with the challenge of providing the first response in life-critical circumstances. The ability to create the right situational awareness and reliable communication with each other are the most important issues between the PPDR, military and voluntary services.

The West Finland Coast Guard District has its own main situation and command center in Turku and it is called the Command and Maritime Rescue Coordination Centre (MRCC Turku). The approach of this case study handles mainly the West Finland Coast Guard District and the Command and Maritime Rescue Coordination Centre and their relationship to each other's situation centers and emergency response centers.

This case study is carried out with the guidance of Yin (2014). The case study illustrates the attempt to produce profound and detailed information about the object being researched. The materials collected for this case study are based on observations, interviews, scientific publications, collected articles and literary material. Interviewees were chosen on the basis of their expertise in their specialist roles: they operate or have operated in public safety organizations. One of the interviewees has been a technical developer in public safety organizations. The interviews were recorded and analyzed using the qualitative content analysis method.

The case study's empirical research approach is due to the fact that the researcher had to study more deeply the culture of the situational centers and the actual working environment of employees working in the field. Participant observation makes it possible to get close to the actors.

4. Case study findings

The Finnish Border Guard uses mainly Virve telephones for communication between authorities, but VHF and MF connections are also widely used in the coastal area. They have a direct emergency number for emergency situations. In addition, the emergency calls placed by citizens can be redirected from the Emergency Response Centers to the MRCC Turku. Their own command and control center (the Command and Maritime Rescue Coordination Centre) reserves cooperation in multi-authority situations if a long-standing major accident occurs. In a situation such as this, managerial personnel such as a rescue manager or a police field manager meet in the control and command room to work with each other. The Command and Maritime Rescue Coordination Centre (MRCC Turku) is their management and marine rescue center. The management relationships may be unclear in such cases, therefore it is important to meet. Different authorities do not receive real time information about available aid from voluntary associations, not even the Maritime Rescue Coordination Centre.

The West Finland Coast Guard District is responsible for security in the whole sea area in Western Finland. They have a situation and analysis team that is there for half of the day. The same group has three customs officers who work with them daily. It is a daily operational mode.

The area of operations of the West Finland Coast Guard District covers the emergency area of four emergency centers. Virve has only a maximum of 20 call groups per workstation. This means that the monitored area is quite wide and one major accident will relocate resources from daily routine to a more serious accident. It is possible to control all the groups that they want with one terminal device, but they have to share the groups

between the different workstations. This procedure helps them better analyze events. The field commander and officer in charge of rescue operations decide together if it is necessary to issue a major accident alert. The coast guard does not have a shared situational awareness system for cross-border cooperation. Currently, the situational picture of an individual patroller is based on the Virve communications and background information that has been collected before via radio communication, for example. There is no possibility to use visual real time data communication systems, but the surveillance aircraft has a good camera that records events and transfers data to the MRCC. The use of real time video is not currently possible. The flow of real time data is not transmitted, for example, from cruise ships or from patrol vessels to the Maritime Rescue Coordination Centre. Small ships or boats that are attempting to cross the Schengen border create additional challenges, especially in situations where the transponders are switched off. They have a certain number of cameras in the archipelago and in places they support border control. The cameras allow tracking and identifying which ships are operating there. Underwater surveillance is carried out in cooperation with the Finnish Navy.

Operational field work covers statutory tasks involving the leading positions of other authorities as provided by the law on the Border Guard (Border Guard Act) such as executive assistance tasks and the management of Maritime Rescue. It includes, for example, that oil spills and initial actions for the fight against oil spills belongs nationwide to them, also in the Gulf of Finland. Concerning sea rescue, international contacts are handled in neighboring countries and, as the case may be, more broadly. A special function is the coordination of the entire Finnish Border Guard's flight operations as appropriate. Airbase stations are located in Helsinki, Rovaniemi and Turku.

In Turku, there is also a surveillance aircraft. Aviation operations are coordinated by a field commander in Turku. If the Gulf of Finland coast guard has a sea rescue mission, they can use aerial vehicles in Helsinki. Helicopters are widely used by other authorities in their tasks, such as to transfer patients to hospitals and to search for fire. They practice and participate in multiauthority exercises, major accident exercises and rescue exercises. There are several maritime rescue authorities in Finland that, using their own special expertise, take part in the task and, accordingly, border control takes part in other tasks and helps with the equipment if necessary.

5. Discussion

Computing technology in most control centers, situational centers and emergency response centers is based on sequential computing and the infrastructure based on human capabilities and activities. To support the next-generation hybrid smart control center monitoring, analysis and control functions, the parallel computing infrastructure needs to be implemented with proper prioritizing and scheduling different real time simulation tasks.

Government agents, utility executives, policymakers and technology providers must agree on a common goal and take actions to accelerate the process towards final deployment, and legal and organizational barriers have to be removed. Given the scale of the effort required and the enormity of the challenges ahead, collaboration among different sectors is essential and should be developed through various channels in order to ensure and accelerate the success of the future smart control centers.

6. Conclusion

Limited data transmission and the lack of visual real time data capabilities prevent the formulation of an accurate situational picture in MRCC Turku. Coast Guard patrols cannot share real time information with other patrols or the MRCC Turku. There is a need to strengthen the entire maritime intelligence ecosystem. The greatest need for new sensor technology is at sea (Lemponen, 2012). There is also a need in command and control functions to design a combination of a new kind of hybrid sensor technology that uses OSINT tools in order to detect threats in advance because a cyber situational picture is needed. For example, drug trafficking can be prevented by more effective hybrid-based intelligence.

Effective cooperation between security authorities needs a common technology for all authorities. Municipal actors relying on municipal technical resources is not sustainable because cooperation between the Finnish Border Guard and emergency services has developed, especially at the site of the scene of maritime accidents. Organizational cooperation requires a common infrastructure and clearer and faster connections. The DSiP telemeter includes mobile communication, IT systems and a command and control center. The DSiP solution is already in use with the Finnish Border Guard, but its potential could be better utilized (Hult, 2012).

Open source intelligence is an applicable emergency response tool for public safety authorities. The presented hybrid model will offer an updated emergency response management model to PPDR services. Currently, new information systems are already out of date when they are introduced.

A dynamic cyber-physical ecosystem or infrastructure is needed in order to respond to a rapidly evolving maritime alert situation. It is obsolete to manage public safety organizations as separate public safety actors. The internal and external security atmosphere can no longer be separated in the traditional sense. Threats have changed into combinations of threat types and, as a consequence, public safety organizations like the Finnish Border Guard must be able to prevent new kinds of hybrid threats and respond to them. Improving the flow of information between the public sector and citizens, including volunteer associations, is also a relevant part of this framework. It must be possible to prevent and respond faster to the realization of threats. A modelling platform for a smart emergency response model can lead to important new results. The cyber domain can be used as a powerful dimension to enhance data fusion to more accurate overall situational awareness. By processing raw data on anomalous behavior in advance, PPDR services can use smart emergency response functions before any threats have occurred, as illustrated in Figure 3.

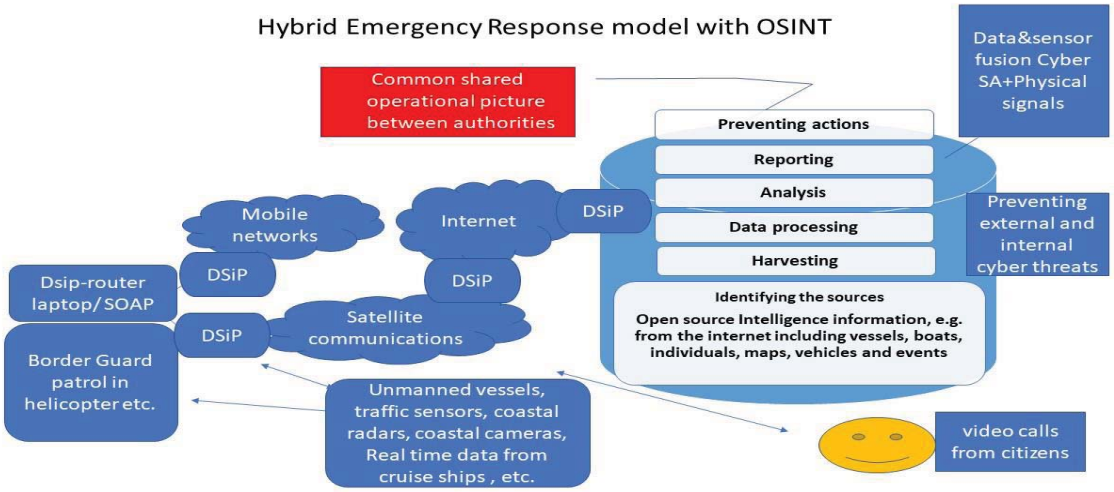

Figure 3: Hybrid Emergency Response model with OSINT

The next generation hybrid model will integrate existing surveillance systems and networks with new ones and give all concerned authorities access to the information they need for their missions at sea. Combining pieces of open source information to ensure correct and reliable information is shared is of primary importance. The essential information is processed in the desired form for the accident site command center. The next generation emergency response system is based on active operations and automated functions. At the very least, a direct communication connection without unnecessary intermediaries must exist from the situation center to the government situation center.

References

Act on Cooperation between the Police, Customs and the Border Guard, 687 (2009).

Border Guard Act, 578 (2005).

Border Guard Administration Act, 577U.S.C. (2005b).

The Border Guard in Figures - the Finnish Border Guard. Retrieved from https://www.raja.fi/facts/the_border_guard_in_figures

CBRNE strategy working group. (2017). National CBRNE strategy 2017. (No. 32). Ministry of the Interior.

Cospas-Sarsat Programme (2016). Cospas-Sarsat system data. (No. 42). Canada: Secretariat of the International Cospas-Sarsat Programme.

Dos Passos, D. (2016) “Big data, data science and their contributions to the development of the use of open source intelligence. Systems & Management, 11 p 392–396

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. Proceedings of the Human Factors Society 32nd Annual Meeting, 97–101.

Finnish Border Guard and Finnish Transport Safety Agency. (2016). Baltic Sea MIRG - European maritime traffic risk assessment on ship fires. Ministry of the Interior.

The Finnish Border Guard. (2018) Finnish Border Guard maritime SAR suitable equipment. Retrieved from http://www.raja.fi/sar/en/equipment

The Finnish Border Guard. (2017). According to the website: https://www.raja.fi/projects/horizon2020 Ministry of the Interior.

Franke, U. and Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. Computers & security (pp. 18-31-46 DOI 10.1016/j.cose.2014.06.008

Glassman, M., & Kang, M. J. (2012). "Intelligence in the internet age: The emergence and evolution of open source intelligence (OSINT)", Computers in human behaviour, 28, pp 673–682.

Homeland Security. (2008) National response framework. Washington, DC: FEMA publications warehouse.

Hult, T. (2012) Public Protection and Disaster Relief services ICT-systems developing and integration. Thesis

Kaukanen, J. and Möttönen, M. (2010) Border guard headquarters - MARITIME SEARCH AND RESCUE MANUAL 2010. Ministry of the Interior.

Lemponen, I. (2012) Vedenalainen datasiirto – langallisten ja langattomien tiedonsiirtojärjestelmien nykytila ja kehitysnäkymät. http://www.doria.fi/bitstream/handle/10024/85020/Lemponen_IM.pdf?sequence=1

MARISA. (2018) "MARISA - Maritime Integrated Surveillance Awareness" [online], Marisa Project, https://www.marisaproject.eu/

The Maritime Search and Rescue Act, 1145U.S.C. (2005a).

Ministry of Defence. (2010) Security strategy for society, government resolution. Helsinki: Ministry of Defence

Morrow, J. and Odierno, R. (2012) Open source intelligence, ATP 2-22.9, army techniques publication. Washington: Headquarters, Department of the U.S. Army.

National Protection and Programs Directorate (NPPD). (2011) Enabling Distributed Security in Cyberspace - Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. United States: Department of Homeland Security.

Nurmi, P. (2015) OSINT - avointen lähteiden internet -tiedustelu. Helsinki: Aalto yliopisto.

ISI. (2017) Kingfisher – multi sensor, multilayer, maritime intelligence system. Retrieved from https://www.imagesatintl.com/solutions-services/maritime-situational-awareness/

Rajamäki, J. and Villemson, T. (2009). Designing emergency vehicle ICT integration solution. Proceedings of the 3rd International Conference on Communications and Information Technology, Athens, Greece. 83–90.

SIME. (2014) Mapping shipping intensity and routes in the Baltic Sea using historical AIS data. (No. 5). Göteborg: Havsmiljöinstitutet.

Simola, J. and Rajamäki, J. (2015) How a real time video solution can affect the level of preparedness in situation centres. Paper presented at the Second International Conference on Computer Science, Computer Engineering and Social Media (CSCESM), Lodz, Poland. https://doi.org/10.1109/CSCESM.2015.7331824

Simola, M., Aheristo, M., and Puustinen V. (2015) Vartiolaiva Turva tilannekuvan tuottajana- Rannikon Puolustaja

Trottier, D. (2015) "Open source intelligence, social media and law enforcement: Visions, constraints and critiques." European Journal of Cultural Studies, 18, pp 530–547.

Vetter, M. (2015) Open source intelligence techniques and the dark web Retrieved from www.itproportal.com/2015/10/30/open-source-intelligence-techniques-and-the-dark-web/

Wood, M. Graham. (2016) Social media intelligence, the wayward child of open source intelligence.

Yin, R. K. (2014) Case study research, design and methods (5th ed.). Thousand Oaks: Sage Publications.